



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,493	07/06/2001	Michael Freed	NEXSI-01111US0	4137
28863	7590	01/04/2005	EXAMINER	
SHUMAKER & SIEFFERT, P. A. 8425 SEASONS PARKWAY SUITE 105 ST. PAUL, MN 55125			ALOMARI, FIRAS B	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/900,493

Applicant(s)

FREED ET AL.

Examiner

Firas Alomari

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on 06 July 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) 15 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>0311/2004</u> .   | 6) <input type="checkbox"/> Other: _____                                    |

## DETAILED ACTION

### ***Specification***

1. The Specification is objected to because of the following informalities:

line 14 of page 4 "ach" should be "each"

line 10 of page 11 "TCI/IP" should be "TCP/IP"

lines 6 and 7 of page 11 refer to a co-pending patent application without listing the application number and the inventors.

Appropriate correction is required.

### ***Claim Objections***

2. Claim 15 objected to because of the following informalities: is on the 2nd

line should be changed to if. Appropriate correction is required.

### ***Double Patenting***

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Art Unit: 2136

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1-5, 7-13 and 15-19 are provisionally rejected under the judicially created doctrine of double patenting over claims 1-30 of copending Application No. 09900496. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

5. Claims 1-5, 7-13 and 15-19 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1-30 of copending Application No. 09900496 in view of Narad US (6,157,955). \*\*\*

This is a provisional obviousness-type double patenting rejection.

- As to independent claim 1 of this application, claim 1 of the '496 application is a corresponding claim. Claim 1 of the '496 application does not explicitly explain a packet authentication. However Narad teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7) to verify the validity of the data packets. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to add the authentication step from Narad to authenticate received packets after the final packet in the data segment received. One would be motivated to

Art Unit: 2136

do so in order to identify and discard packets that have been altered or modified.

6. As to claim 2 of this application, '496 application doesn't explain a forwarding data which spans over multiple TCP segments. However the examiner deeming this to be inherent to any TCP/IP and SSL communication system, which split the application data packets to multiple TCP/IP packets to be transmitted over the network.

7. As to claim 3 in this application, claim 20 of the '496 application is a corresponding claim.

8. As to claim 4 in this application, claim 20 of the '496 application is a corresponding claim.

9. As to claim 5 in this application, claim 7 of the '496 application is a corresponding claim.

As to the remaining claims, the reasons for this provisional rejection should be obvious from the discussion of claims 1,2 and 3 and the similarity between the claims of the two applications.

### ***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to

Art Unit: 2136

be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin US (6,681,327) in view of Narad US (6,157,955).

As per claims 1: Jardin disclose

A method for enabling secure communication between a client on an open network and a server apparatus on a secure network (item 100 of FIG. 1), the method performed on a intermediary apparatus coupled to the secure network and the open network (item 120 of FIG. 1), comprising:

- Negotiating a secure communications session with the client apparatus via the open network;( items 210, 220, 230 and 240 of FIG 2; describes the "handshake " between the client and the server which used to start any communication between the server and the client)
- Negotiating an open communications session with the server via the secure network; (Col 6, lines 40-46)
- Receiving encrypted packet application data having a length greater than a packet length via multiple data packets; (Col 6, line 67; The examiner deeming this to be inherent to any TCP/IP system, which split the application data packets to multiple TCP/IP packets to be transmitted over the network.)
- Decrypting the encrypted packet application data in each data packet; (Col 6, line 67)

Art Unit: 2136

- Forwarding decrypted, unauthenticated application data to the server via the secure network; (Col 7, line 4)
- Authenticating the decrypted packet data on receipt of a final packet of the segment. / Jardin do not explicitly explain a packet authentication.

However Narad teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7) to verify the validity of the data packets. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Jardin with the teaching of Narad to authenticate received packets after the final packet in the data segment received. One would be motivated to do so in order to identify and discard packets that have been altered or modified.

As per claim 2: Jardin system discloses

- Forwarding data which spans over multiple TCP segments. (Col 7, lines 44-45)

As per claims 3 and 10: Jardin system discloses

- The method of claim 2 wherein said data is not buffered during decryption. (Col 3, lines 4-13 / in one embodiment the first server is configured to decrypt contents of the data packet and re-direct the data packet)

As per claim 4, 11 and 12: Jardin system discloses

- The method of claim 2 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data (Col 2, lines 65, through Col 3, line 3 / the broker in the second embodiment have dynamically allocated buffer)

As per claims 5 and 19:

- Authenticating the decrypted data after a final segment of multi segment encrypted data stream is received. / Jardin do not explicitly explain a packet authentication. However Narad teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7) to verify the validity of the data packet. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Jardin with the teaching of Narad to authenticate received packets after the final packet in the data segment received. One would be motivated to do so in order to identify and discard packets that have been altered or modified.

As per claims 6,14 and 20:

- Notifying the client apparatus if a failure in said step of authenticating occurs. The examiner deeming this to be inherent to any SSL based communication systems that utilize an alert protocol that handles all SSL crypto related errors. The "bad\_record\_mac " error notifies the client if the MAC of the received SSL record is incorrect.



As per claim 7:

A method for processing encrypted 'data transferred between a first system and a second system, comprising:

- Providing an accelerator device including a decryption engine in communication with the first system via an open network and the second system via a secure network;( item 120 of FIG. 100)
- Receiving encrypted data from the first system via the open network in the form of application data spanning multiple packets, each packet having a packet length and information for authenticating the application data;( Col 6, line 67)
- Decrypting ones of said packets as said packets are received, (Col 7 lines 39-41)
- Forwarding application data as said packets are decrypted to the second device via the secure network; (Col 7, line 4)
- Authenticating the data when said information for authenticating the data is received in a last of said multiple packets. Jardin do not explicitly explain a packet authentication. However Narad teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7) to verify the validity of the data packet. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Jardin with the teaching of Narad to authenticate received packets after

Art Unit: 2136

the final packet in the data segment received. One would be motivated to do so in order to identify and discard packets that have been altered or modified.

As per claim 8: Jardin system teaches

- The method of claim 7 wherein said step of receiving comprises receiving SSL encrypted data. (Col 4, lines 11-12)

As per claims 9,13,17 and 18: Jardin system teaches

- The method of claim 7 wherein said step of decrypting comprises decrypting application data encrypted using SLL, DES and a 3DES algorithm. (Col 5, lines 16-20)

As per claim 15:

- The method of claim 7 wherein said step of authenticating includes generating a reset to the second device if said step of authenticating fails.  
The examiner is deeming this to be inherent to any SSL communication system, where the authentication failure error message "bad\_record\_mac " in the SSL protocol is considered fatal and upon receive of the message connection is closed.

As per claim 16: Jardin system teaches

Art Unit: 2136

A method of providing secure communications using limited buffer memory in an secure sockets layer processing device (Col 6, lines 5-11), comprising:

- Receiving SSL encrypted data having a length greater than a TCP segment carrying said data;( Col 6, line 67)
- Buffering the SSL encrypted data in a memory buffer in the SSL accelerator device, the buffer having a length equivalent to the block cipher size necessary to perform the cipher;(Col 6, lines 9-14)
- Decrypting the buffered segment of the received SSL encrypted data to provide decrypted application data;( Col 7 lines 39-41)
- Forwarding the decrypted application data to a destination device. (Col 7, line 4)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on Mon-Fri.

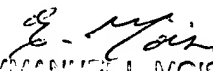
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari  
Art Unit 2136

FA

  
EMMANUELLE L. NOISE  
PRIMARY EXAMINER